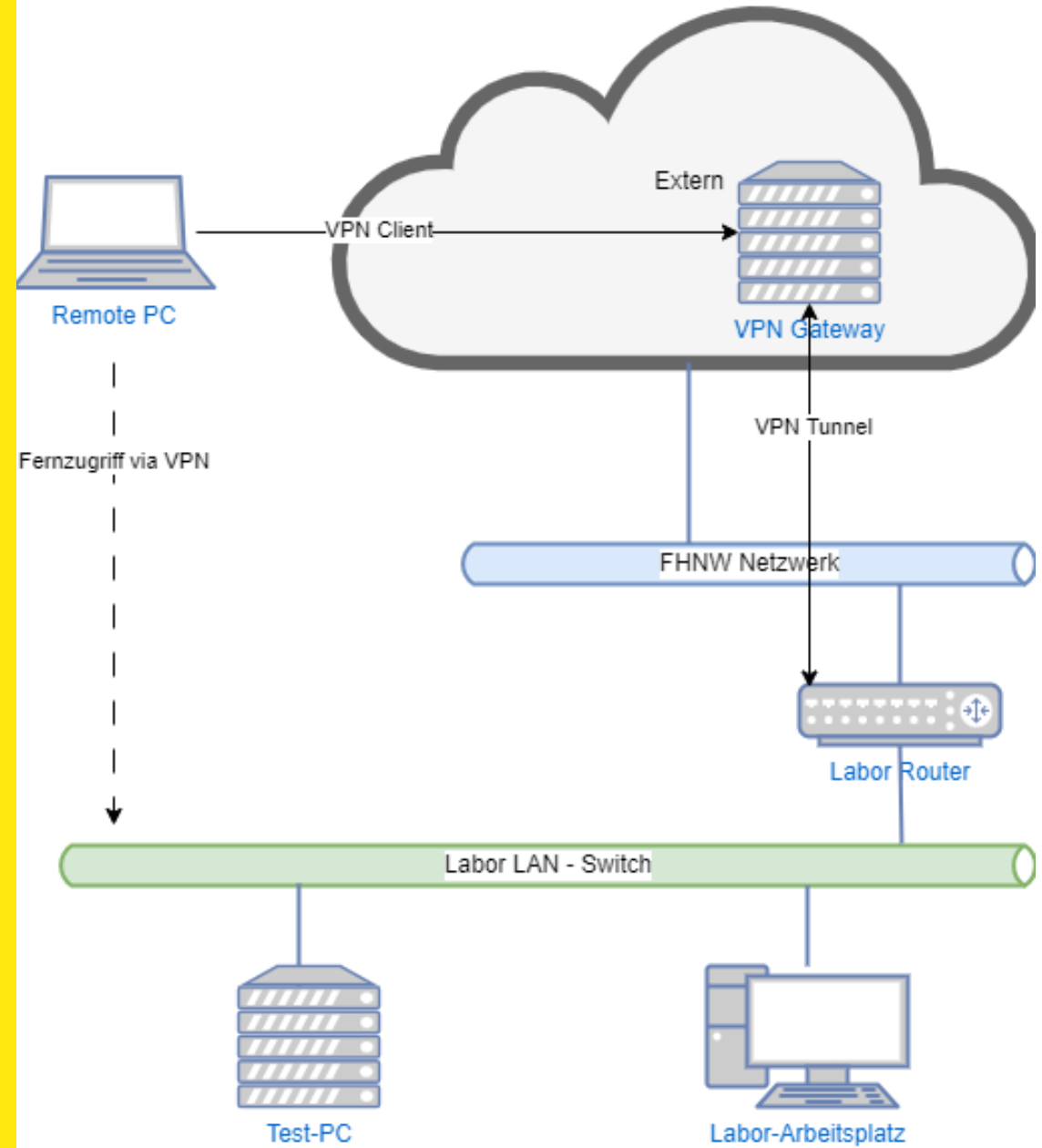


Lab Connector – Fernzugriff auf Laboraufbauten

IMVS Tech Talk

Matthias Krebs

15. Mai 2024



Inhalt

1. Einführung und Anwendungsfälle
2. Frühere Lösungsansätze
3. Lab Connector

Einführung und Anwendungsfälle

Herausforderung

In Projekten, in denen mit Hardware gearbeitet wird, muss ggf. ein ganzes Labor-LAN ans Netzwerk angebunden werden.

Das kann aufwendig sein, sobald mehr als ein einzelnes Gerät involviert ist → Prozesse der Corporate IT

Ziel

- Universelle Lösung für die Verwendung in unterschiedlichen Projekten

Anforderungen

- Niedrige Hardware-Kosten
- Flexibler Netzwerk-Zugriff, möglichst auch mit Fernzugriff
- Möglichst geringer administrativer Aufwand

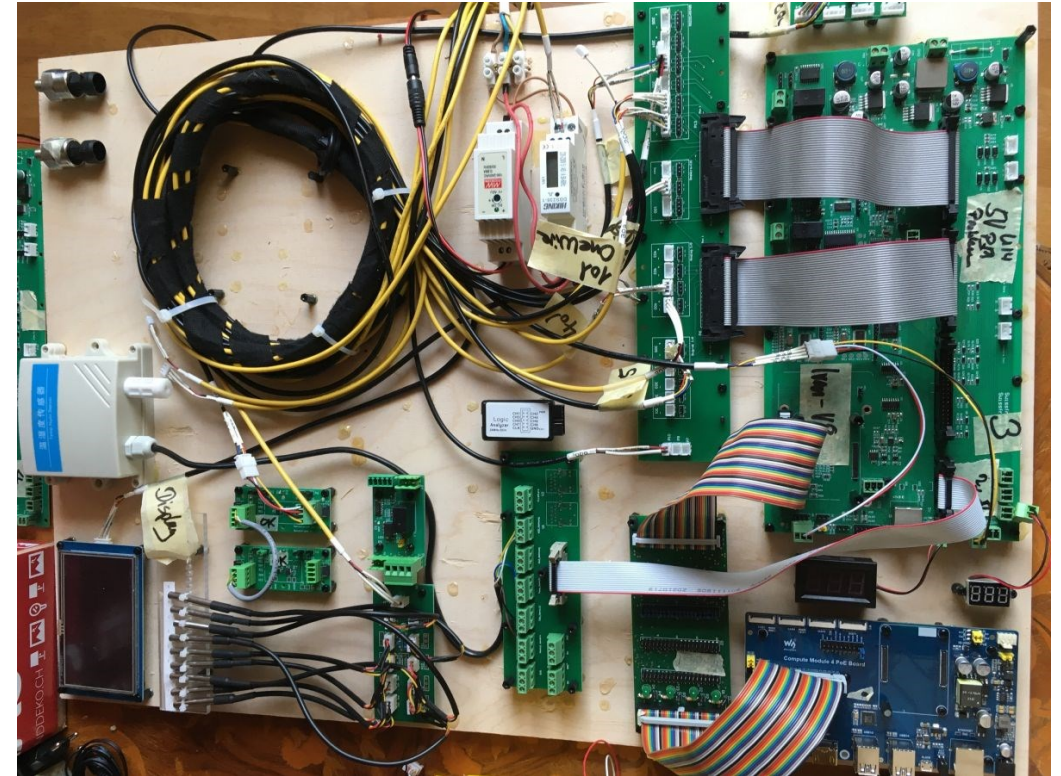
Anwendungsfall 1 – Swissframe

Innosuisse-Projekt bis März 2024, IMVS

Badezimmer-Apparatur für Lüftung und
Warmwassererzeugung, mit IoT-Anbindung

Benötigt ein Labor-LAN mit eigenem DHCP-Server zur
Provisionierung der Embedded-Systeme (RPI
Compute Module)

Vorläufer der Lab-Connector-Lösung



Anwendungsfall 2 – SmartGridready Testlabor

Vom BFE unterstütztes Projekt mit Verein SmartGridready, seit 2024, IA+IMVS

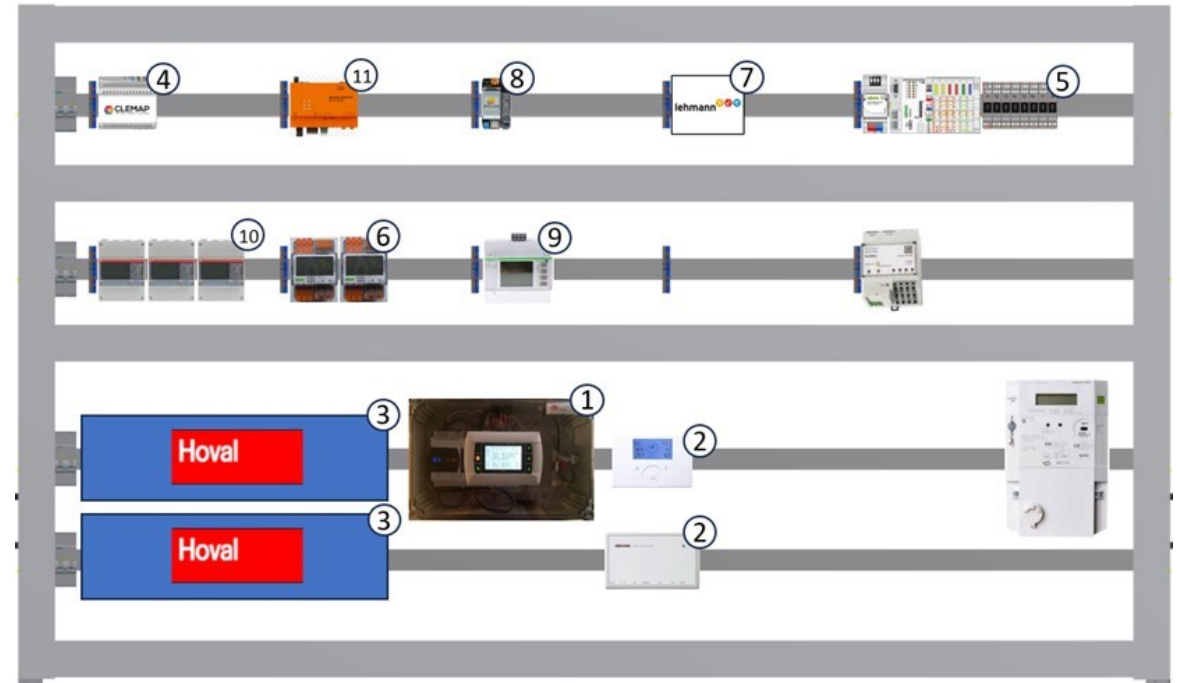
Offener Standard und Software-Stack zur Ansteuerung von Energiezählern, Wärmepumpen, Ladestationen usw.

Testlabor dient Herstellern zur Verifizierung der Kompatibilität mit SGr

Benötigt ein Labor-LAN mit Internetzugang und Fernzugriff, auch für Externe

Erste Anwendung der Lab-Connector-Lösung

www.smartgridready.ch



div. Energie-Messgeräte und -Steuerungen auf Alu-Gestell, meist mit LAN oder WLAN

Frühere Lösungsansätze

Labor-Router im EXP-Netz

Nach Freigabe durch die Corporate IT kann ein Router ins EXP-Netz (für Netzwerkgeräte ohne Authentifizierungsmöglichkeit) eingebunden werden.

Vorteile

- Keine Zugangsdaten nötig, nur MAC-Adresse muss freigeschaltet werden
- Fernzugriff via FHNW-VPN + NAT-Port-Forwarding möglich

Nachteile

- Abgesehen von einigen Standard-Ports müssen alle ein- und ausgehenden Verbindungen explizit freigeschaltet werden
- Kein transparenter Fernzugriff aufs Labor-LAN
- Auf ein Gebäude beschränkt

Labor-Router mit 802.1X

Wenn man einen Router verwendet, welcher 802.1X-Authentifizierung am WAN-Port unterstützt, kann er wie jedes persönliche Gerät ans FHNW-Client-Netzwerk angeschlossen werden.

Alternativ kann ein WLAN-Router als WLAN-Client konfiguriert und ins FHNW-WLAN eingebunden werden.

Vorteile

- Einfacher Zugriff auf FHNW-Netzwerk und Internet – keine Freischaltung nötig
- Funktioniert in jedem Gebäude

Nachteile

- Die meisten einfachen Router können kein 802.1X → nur mit Custom-Firmware machbar, z.B. **OpenWRT**
- Persönliche Zugangsdaten hinterlegt
- Zugriff auf interne FHNW-Ressourcen – evtl. nicht erwünscht
- Kein Fernzugriff möglich – auch nicht via FHNW VPN

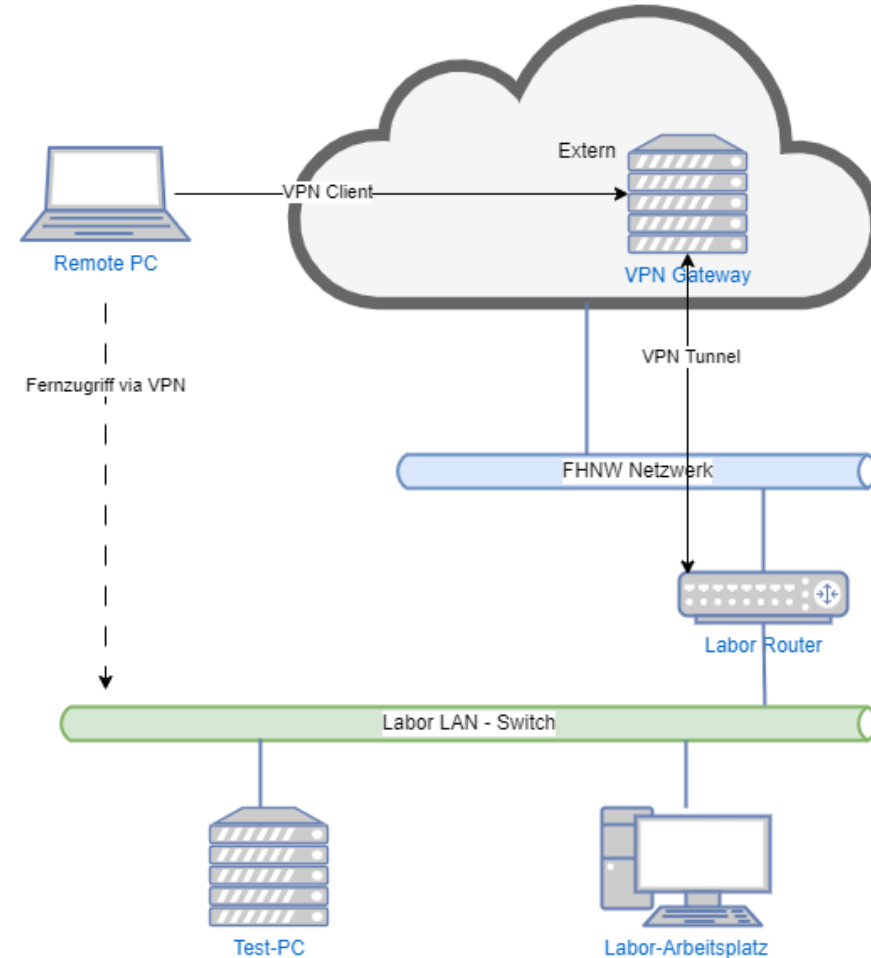
Lab Connector

Lab Connector – Überblick

Konzept

- Wireguard VPN
- VPN Gateway in Public Cloud
- Labor-Router baut VPN-Tunnel als Client auf → Internetzugang und Fernzugriff
- Remote-User verbinden sich mit VPN-Gateway → Zugriff auf Labor-LAN via VPN-Tunnel

- Mischung aus «Road Warrior» und «Site-to-Site»
- Router braucht nur ausgehende Verbindung – funktioniert auch hinter NAT



Lab Connector – VPN Gateway

OPNSense 24.1

- Open-source Router/Firewall
- Für PCs und Embedded-Systeme
- FreeBSD
- Wireguard VPN integriert

<https://opnsense.org/>

The screenshot displays the OPNSense 24.1 dashboard for a system named 'lab-connector.cs.technik.fhnw.ch'. The dashboard is organized into several sections:

- System Information:** Shows system details such as Name, Versions (OPNsense 24.1.6-amd64, FreeBSD 13.2-RELEASE-p11, OpenSSL 3.0.13), Updates (with a 'Click to check for updates' link), CPU type (Intel Xeon Processor (Skylake, IBRS) (2 cores, 2 threads)), CPU usage (100%), Load average (0.20, 0.23, 0.23), Uptime (31 days 23:07:08), Current date/time (Wed May 15 6:22:43 UTC 2024), Last config change (Tue May 14 15:48:03 UTC 2024), and resource usage bars for CPU (0%), State table size (0% (5/201000)), Mbuf usage (1% (1254/125322)), Memory usage (26% (537/2010 MB)), and Disk usage (14% / [ufs] (2.5G/19G) and 1% /boot/efi [msdosfs] (1.7M/256M)).
- Services:** A table listing various services with their descriptions and status indicators (play, stop, refresh icons).

Service	Description	Status
configd	System Configuration Daemon	▶ ⏏
cron	Cron	▶ ⏏
dhcpcd	DHCPv4 Server	▶ ⏏
login	Users and Groups	▶ ⏏
ntpd	Network Time Daemon	▶ ⏏
openssh	Secure Shell Daemon	▶ ⏏
pf	Packet Filter	▶ ⏏
routing	System routing	▶ ⏏
sysctl	System tunables	▶ ⏏
syslog-ng	Syslog-ng Daemon	▶ ⏏
unbound	Unbound DNS	▶ ⏏
webgui	Web GUI	▶ ⏏
wireguard	WireGuard sgr-testlab	▶ ⏏
wireguard	WireGuard test	▶ ⏏
- Gateways:** A table showing gateway status.

Name	RTT	RTTd	Loss	Status
WAN_GW 10.0.0.1	~	~	~	Online
- Interfaces:** A table listing network interfaces.

Interface	Speed	Link	IP Address
LAN	10GbBase-T <full-duplex>	↑	192.168.1.1
WAN	10GbBase-T <full-duplex>	↑	10.0.0.108
WpSGrTestlab	↑		198.18.1.1
WpTest	↑		198.18.2.1

VPN Gateway in Cloud aufsetzen

Lab Connector VPN Gateway wird in einer Public Cloud (hier SwitchEngines) installiert.

Kein vordefiniertes Image für OPNSense in SwitchEngines vorhanden.

Lösung

Zuerst eine OPNSense VM lokal aufsetzen (z.B. VirtualBox) und als RAW-Image exportieren. Dieses kann in SwitchEngines importiert werden.

Konfigurationsanpassungen vor dem Export

- das Admin-Webinterface muss auch via WAN-Port erreichbar sein → Public IP kann in SwitchEngines nur einem Interface mit Route ins Internet zugewiesen werden
- HTTP_REFERER Check muss deaktiviert sein → wegen Public IP Mapping

Cloud-Netzwerk für VPN Gateway

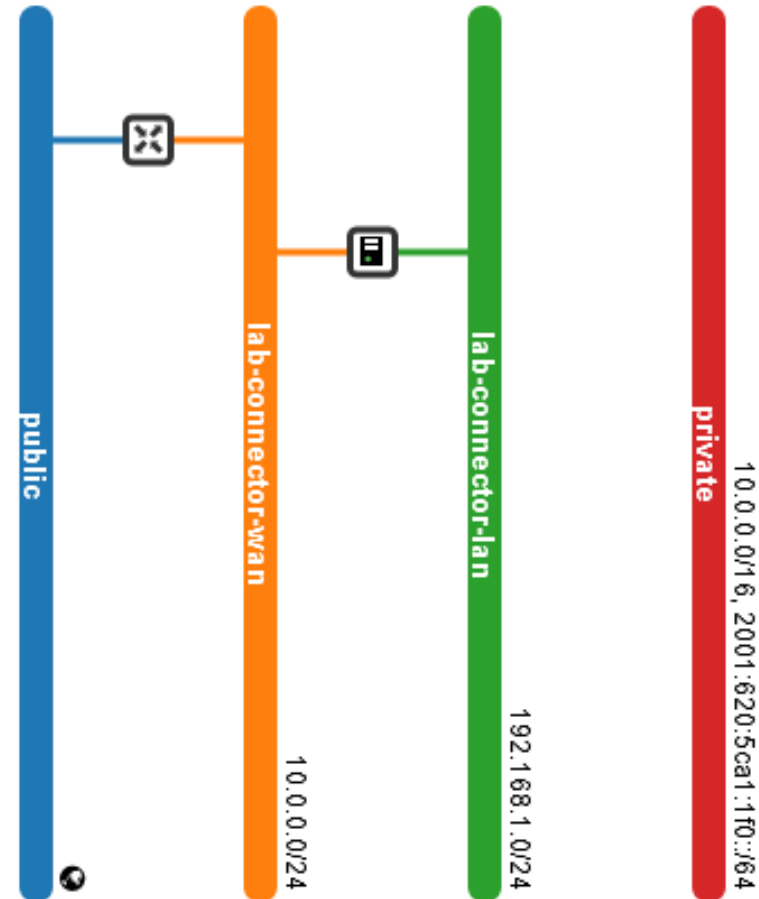
VPN Gateway wird wie ein herkömmlicher NAT-Router konfiguriert:

- 1 LAN (nicht benötigt, muss aber vorhanden sein)
- 1 WAN (Internet und externer Zugriff)
- N VPNs (nur intern auf GW)

1 Public IP Mapping

ext. Zugriff auf WAN-Adresse, Admin-Interface

Aktuell nur IPv4 – später evtl. auch IPv6



Einrichten eines neuen Labor-VPN

In OPNSense

1. Eine neue **Wireguard**-Instanz erstellen
2. Parameter einstellen
 - Schlüssel
 - UDP-Port
 - Tunnel-Adresse (internes VPN-Subnet)
3. Interface erstellen und zuweisen
4. Firewallregeln erstellen
5. Clients erstellen (Peers)
 - 1 Labor-Router, mit Route ins Labor-LAN
 - N Clients für Remote-Zugriff

Konflikte bei Port, VPN-Subnet und Labor-LAN vermeiden!

The screenshot shows the 'Edit instance' configuration page in OPNSense. The page is titled 'Edit instance' and has a close button (X) in the top right corner. Below the title, there is a 'full help' link. The configuration is organized into several sections:

- advanced mode** (toggle on)
- Enabled** (checkbox checked)
- Name** (text input: test)
- Instance** (text input: 1)
- Public key** (text input: ife7aWybWbZGKH5lpgn3BTQitpyskAq9Hm7Ny7T6Z ...)
- Private key** (text input: eEBxmkKhwp/mb5mfBL9HI04bax3E5vWk/dvulcEIEG=)
- Listen port** (text input: 51822)
- MTU** (text input: empty)
- DNS servers** (text input: empty, with 'Clear All', 'Copy', 'Paste', and 'Text' buttons below)
- Tunnel address** (text input: 198.18.2.1/24, with 'Clear All', 'Copy', 'Paste', and 'Text' buttons below)
- Depend on (CARP)** (dropdown menu: None)
- Peers** (dropdown menu: Nothing selected, with 'Clear All' button below)
- Disable routes** (checkbox unchecked)
- Gateway** (text input: empty)

At the bottom right, there are 'Cancel' and 'Save' buttons.

Firewallregeln

VPNs sollen gegeneinander isoliert werden

Quellen

- VPN-Subnet
- Labor-LAN

Ziele

- ANY (Internetzugriff)
- Labor-LAN (oben enthalten)

Firewall: Rules: WgTest Select category Inspect

<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	<input type="checkbox"/>
<i>Automatically generated rules</i> 15									
<input type="checkbox"/>	IPv4 *	WgTest net	*	*	*	*	*		<input type="checkbox"/>
<input type="checkbox"/>	IPv4 *	172.16.234.0/24	*	*	*	*	*		<input type="checkbox"/>

pass block reject log in first match
 pass (disabled) block (disabled) reject (disabled) log (disabled) out last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

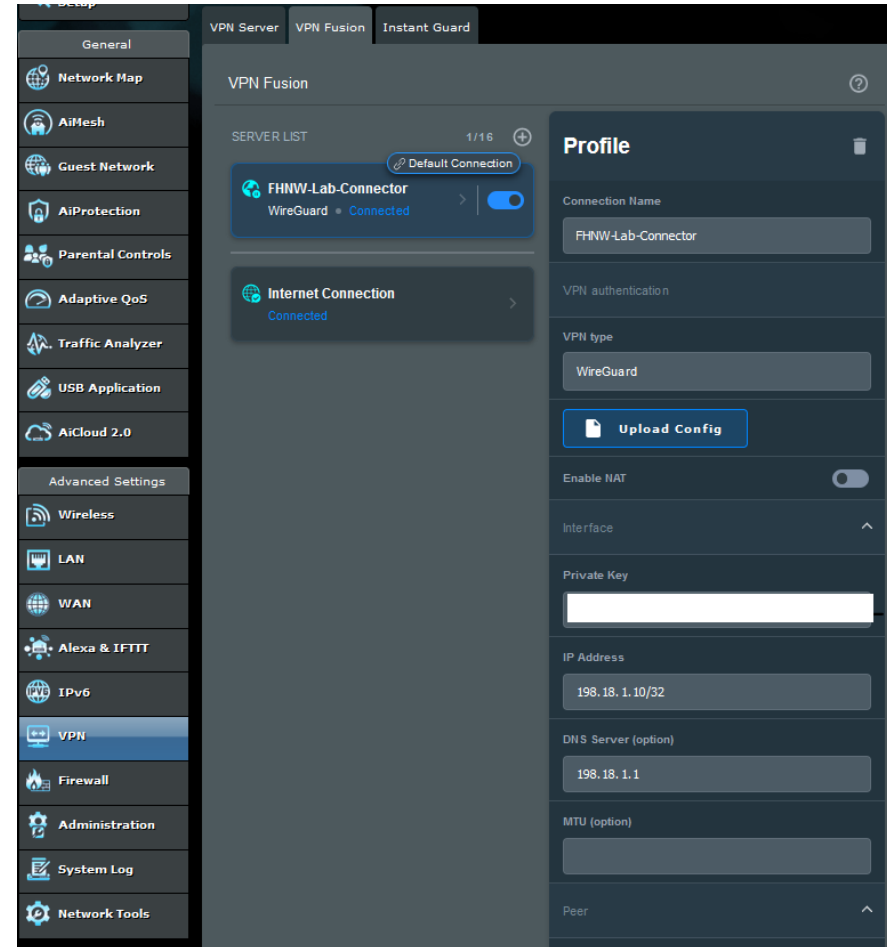
WgTest rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

Lab Connector – Labor-Router

Jeder Router möglich, der **Wireguard** als **Client** unterstützt

ASUS RT-AX58U

- Wireguard Client out of the box (VPN Fusion)
- kann gesamten Traffic durch VPN leiten
- Auch für site-to-site geeignet



VPN Client für Labor-Router konfigurieren

In OPNSense Peer konfigurieren

- Schlüssel
- Bei AllowedIPs muss Labor-LAN ergänzt werden
→ wird über diesen Peer geroutet

Labor-LAN kann immer nur über 1 Peer geroutet werden!

Auf dem Router

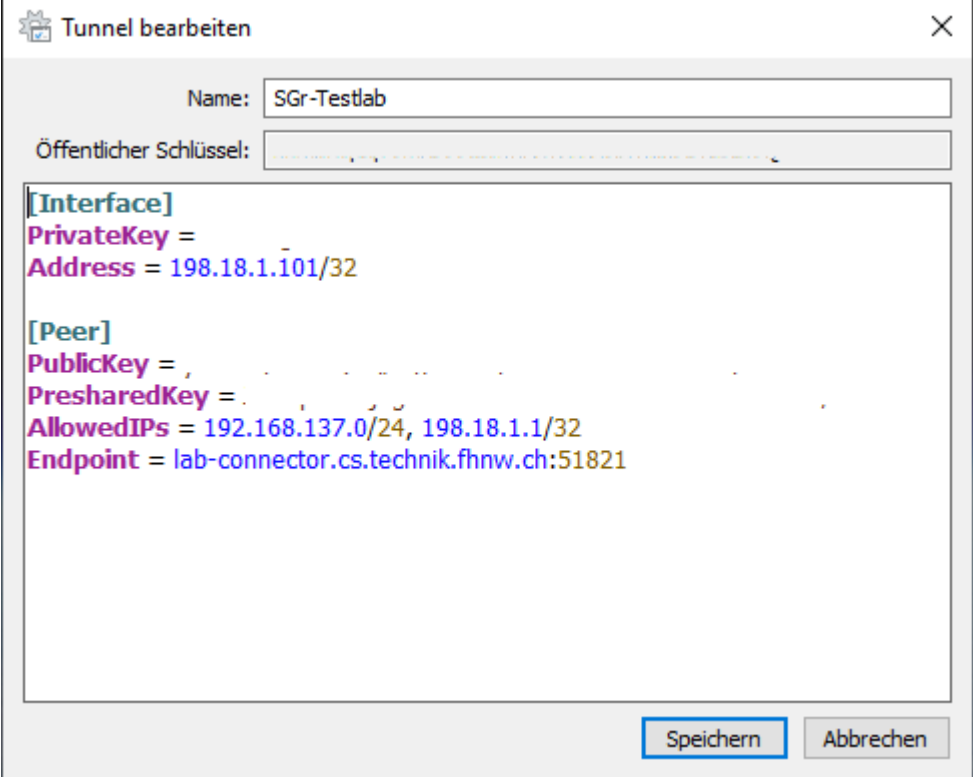
- Endpoint
- Schlüssel
- Bei AllowedIPs 0.0.0.0/0 eintragen → gesamten Traffic via VPN routen

Edit peer

Enabled	<input checked="" type="checkbox"/>
Name	<input type="text" value="test-connector"/>
Public key	<input type="text" value="blOC71rcTQCkDpH+NqV5h258rMXNN3uqRL2Wgd+a ..."/>
Pre-shared key	<input type="text" value="75iuOMuuAdyBgfolq/cdNZtlnQMYZ5Wc4RhvzUJ4ymw="/>
Allowed IPs	<input type="text" value="198.18.2.10/32 ×"/> <input type="text" value="172.16.234.0/24 ×"/> ✖ Clear All 📄 Copy 📄 Paste 📄 Text
Endpoint address	<input type="text"/>
Endpoint port	<input type="text"/>
Instances	<input type="text" value="test"/> ✖ Clear All
Keepalive interval	<input type="text" value="25"/>

VPN Client für Remote-Zugriff konfigurieren

- Endpoint (VPN Gateway)
- Public + Private Keys
- VPN-Adresse – i.d.R. fix pro Client
- AllowedIPs bestimmt die Routen des Clients
- Labor-LAN
- VPN-Adresse des Gateway (optionaler DNS)



The screenshot shows a configuration window titled "Tunnel bearbeiten" with a close button (X) in the top right corner. The window contains the following fields and text:

- Name:** SGr-Testlab
- Öffentlicher Schlüssel:** [Empty field]
- [Interface]**
 - PrivateKey =** [Empty field]
 - Address =** 198.18.1.101/32
- [Peer]**
 - PublicKey =** [Empty field]
 - PresharedKey =** [Empty field]
 - AllowedIPs =** 192.168.137.0/24, 198.18.1.1/32
 - Endpoint =** lab-connector.cs.technik.fhnw.ch:51821

At the bottom right of the window, there are two buttons: "Speichern" (Save) and "Abbrechen" (Cancel).

Zusammenfassung – Ablauf

1. Vorabklärung
 - Adressierung (Labor-LAN)
2. Passenden Router organisieren
3. Labor-VPN einrichten lassen
4. Router von Corporate IT freischalten lassen (MAC-Adresse, 1 Zugriffsregel für VPN-Tunnel)
5. Router konfigurieren
6. Remote-Clients einrichten

Ausblick

Zukünftige Erweiterung auf IPv6

Sonstige Ideen für Verbesserungen?